increase security, where users are assigned a secret key that may be stored, for example, on a pocket token or a computer-readable card. Upon attempting to access a desired device or location, a random value, referred to as a "challenge," is issued to the user. The pocket token or computer-readable card then generates a"response" to the challenge by encrypting the received challenge with the user's secret key. The user obtains access to the device or location provided the response is accurate. In order to ensure that the pocket token or computer-readable card is utilized by the associated authorized user, the user typically must also manually enter a secret alphanumeric PIN or password.

In further variations, access control mechanisms have secured access to devices or secure locations by evaluating biometric information, such as fingerprints, retinal scans or voice characteristics. For a more detailed discussion of one such biometric-based access control system, see, for example, United States Patent Number 5,897,616, entitled "Apparatus and Methods for Speaker Verification/Identification/Classification Employing Non-Acoustic and/or Acoustic Models and Databases," United States Patent Application Serial Number 09/008,122, filed January 16, 1998, entitled "A Portable Information and Transaction Processing System and Method Utilizing Biometric Authorization and Digital Certificate Security," and United States Patent Application Serial Number 09/417,645, filed October 14, 1999, entitled "Point of Sale and Vending Service Payment via Portable Communication Device" (Attorney Docket Number YO999-208), each assigned to the assignee of the present invention and incorporated by reference herein.

While such authentication tools reduce the unauthorized access of equipment or a secure facility, they suffer from a number of limitations, which if overcome, could dramatically increase the utility and effectiveness of such tools. For example, there is currently no mechanism to ensure that a person associated with a given password is physically present at the location where the password is utilized. A need therefore exists for an access control mechanism that uses the global positioning system to verify the location of a person who is requesting access to a secured device or location.

In an alternate implementation, biometric identification can be performed over the entire population of potential users. The biometric identification system provides a list of potential names for the user requesting access. The list of top N best matches is then evaluated to determine if any of the users on the list are physically present at the location of the requested device 102, 105. Thus, the identified user must both (i) be listed on the top N list, and (ii) be physically "near" the location of the requested device 102, 105.

It is noted that the present invention is particularly useful for implementing the system described in United States Patent Application Serial Number 09/419647, filed October 14, 1999, entitled "Point of Sale and Vending Service Payment via Portable Communication Device" (Attorney Docket Number YO999-208), assigned to the assignee of the present invention and incorporated by reference above.

It is to be understood that the embodiments and variations shown and described herein are merely illustrative of the principles of this invention and that various modifications may be implemented by those skilled in the art without departing from the scope and spirit of the invention.